C L A I M S

1. An encrypted communication method characterized by comprising the steps of:

a) causing a communication method resolution unit to determine on the basis of a domain name contained in one of a name resolution query transmitted from an application that communicates with a node apparatus connected to a network to resolve an IP address of the node apparatus and a name resolution response as a response to the name resolution query whether the node apparatus is an encrypted communication target node;

b) causing an encrypted communication path setting unit to register the IP address of the node apparatus in an encrypted communication path setting table when the node apparatus is the encrypted communication target node;

c) causing a name resolution query/response transmission/reception unit to transmit the IP address of the node apparatus contained in the name resolution response to the application;

d) causing the application to transmit a data packet in which the IP address of the node apparatus is set as a destination address; and

e) causing a data transmission/reception unit to receive the data packet transmitted from the application and, if a communication partner IP address

set as the destination address of the data packet is registered in the encrypted communication path setting table, encrypt and transmit the data packet.

2. An encrypted communication method according to claim 1, characterized in that processes of the step a, the step b, and the step c are executed by a name resolution proxy unit provided in a node apparatus in which the application operates.

3. An encrypted communication method according to claim 1, characterized in that a process of the step a is executed by a name resolution server, and processes of the step b and the step c are executed by a name resolution proxy unit provided in a node apparatus in which the application operates.

4. An encrypted communication method according to claim 1, characterized in that the communication method resolution unit determines whether the node apparatus is an encrypted communication target node by looking up a setting table in which at least part of the domain name of the encrypted communication target node is registered.

5. An encrypted communication method characterized by comprising the steps of:

a) causing a communication method resolution unit to determine on the basis of a domain name contained in one of a name resolution query transmitted from an application on a client node to resolve an IP

address of another node apparatus serving as a communication target of the application and a name resolution response as a response to the name resolution query whether said other node apparatus is an encrypted communication target node;

b) causing an encrypted communication path setting unit to register, in an encrypted communication path setting table, a correspondence between the IP address of said other node apparatus and an intercept address that is not used in any other communication session when said other node apparatus is the encrypted communication target node;

c) causing a name resolution query/response transmission/reception unit to transmit, to the application as the name resolution response, an intercept address corresponding to the IP address of said other node apparatus contained in the name resolution response;

d) causing the application to transmit a data packet in which the intercept address is set as a destination address; and

e) causing a data transmission/reception unit to receive the data packet transmitted from the application, read out, from the encrypted communication path setting table, a communication partner IP address corresponding to the intercept address set as the destination address of the data packet, set the readout

communication partner IP address as the destination address of the data packet, and encrypt and transmit the set data packet.

6. An encrypted communication method according to claim 5, characterized in that processes of the step a, the step b, and the step c are executed by a name resolution proxy unit provided in a communication encryption node apparatus having the data transmission/reception unit.

7. An encrypted communication method according to claim 5, characterized in that a process of the step a is executed by a name resolution server, and processes of the step b and the step c are executed by a name resolution proxy unit provided in a communication encryption node apparatus having the data transmission/reception unit.

8. An encrypted communication method according to claim 5, characterized in that the communication method resolution unit determines whether said other node apparatus is an encrypted communication target node by looking up a setting table in which at least part of the domain name of the encrypted communication target node is registered.

9. A node apparatus characterized by comprising:

an application that communicates with another node apparatus connected to a network;

a data transmission/reception unit provided in a kernel unit; and

a name resolution proxy unit which relays a name resolution query transmitted from said application to a name resolution server to resolve an IP address of said other node apparatus and a name resolution response as a response to the name resolution query,

said data transmission/reception unit comprising

an encrypted communication path setting table which holds a communication partner IP address, and

a communication encryption unit which receives a data packet transmitted from said application and encrypts and transmits the data packet when a communication partner IP address set as the destination address of the data packet is registered in said encrypted communication path setting table, and

said name resolution proxy unit comprising an encrypted communication path setting unit which registers, in said encrypted communication path setting table, the IP address of said other node apparatus resolved by the name resolution response if it is determined on the basis of a domain name of said other node apparatus contained in one of the name resolution query and the name resolution response that said other node apparatus is an encrypted communication target node.

10. A node apparatus according to claim 9, characterized in that said encrypted communication path setting table holds a plurality of communication partner IP addresses.

11. A node apparatus according to claim 9, characterized in that said name resolution proxy unit further comprises a communication method resolution unit which determines on the basis of the domain name of said other node apparatus whether said other node apparatus is the encrypted communication target node.

12. A node apparatus according to claim 11, characterized in that

said encrypted communication path setting table holds encrypted communication path setting information to be used for communication with a communication partner in correspondence with the communication partner IP address,

said communication encryption unit reads out corresponding encrypted communication path setting information from said encrypted communication path setting table, encrypts the data packet in accordance with the readout encrypted communication path setting information, and transmits the data packet when the communication partner IP address set as the destination address of the received data packet is registered in said encrypted communication path setting table,

said name resolution proxy unit further

comprises a setting table which holds a correspondence between a domain name condition to specify an encrypted communication target node and encrypted communication path setting information,

said communication method resolution unit determines that said other node apparatus is the encrypted communication target node when the domain name of said other node apparatus matches any one of domain name conditions held in said setting table, and

said encrypted communication path setting unit registers, in said encrypted communication path setting table, encrypted communication path setting information corresponding to the matched domain name condition in correspondence with the IP address of said other node apparatus.

13. A node apparatus according to claim 9, characterized in that said name resolution proxy unit further comprises a name resolution query/response transmission/reception unit which transmits, to the name resolution server, the name resolution query transmitted from said application to resolve the IP address of said other node apparatus, receives, from the name resolution server, the name resolution response containing a determination result indicating whether said other node apparatus is an encrypted communication target node and the IP address of said other node apparatus, and transmits, to said application, the name resolution

response containing the IP address of said other node apparatus contained in the name resolution response.

14. A node apparatus according to claim 13, characterized in that

said encrypted communication path setting table holds encrypted communication path setting information to be used for communication with a communication partner in correspondence with the communication partner IP address,

said communication encryption unit reads out corresponding encrypted communication path setting information from said encrypted communication path setting table, encrypts the data packet in accordance with the readout encrypted communication path setting information, and transmits the data packet when the communication partner IP address set as the destination address of the received data packet is registered in said encrypted communication path setting table,

said name resolution query/response transmission/reception unit receives, from the name resolution server, the name resolution response further containing encrypted communication path setting information in addition to the determination result and the IP address of said other node apparatus, and

said encrypted communication path setting unit registers, in said encrypted communication path setting table, encrypted communication path setting information

contained in the name resolution response in correspondence with the IP address of said other node apparatus.

15. A node apparatus according to claim 11, characterized in that said communication method resolution unit determines whether said other node apparatus is an encrypted communication target node by looking up a setting table in which at least part of the domain name of the encrypted communication target node is registered.

16. A communication encryption node apparatus connected, through a network, to a client node apparatus in which an application that communicates with another node apparatus connected to the network operates, characterized by comprising:

a data transmission/reception unit provided in a kernel unit; and

a name resolution proxy unit which relays a name resolution query transmitted from the application to a name resolution server to resolve an IP address of said other node apparatus and a name resolution response as a response to the name resolution query,

said data transmission/reception unit comprising

an encrypted communication path setting table which holds a correspondence between a communication partner IP address and an intercept address, and

a communication encryption unit which receives a data packet transmitted from the application, reads out, from said encrypted communication path setting table, a communication partner IP address corresponding to an intercept address set as a destination address of the data packet, sets the readout communication partner IP address as the destination address of the data packet, and encrypts and transmits the set data packet, and

said name resolution proxy unit comprising

an encrypted communication path setting unit which registers, in said encrypted communication path setting table, a correspondence between the IP address of said other node apparatus resolved by the name resolution response and an intercept address that is not used in any other communication session if it is determined on the basis of a domain name of said other node apparatus contained in one of the name resolution query and the name resolution response that said other node apparatus is an encrypted communication target node, and

a name resolution query/response transmission/reception unit which transmits, to the application as the name resolution response, the intercept address corresponding to the IP address of said other node apparatus contained in the name resolution response received from the name resolution

server.

17. A communication encryption node apparatus according to claim 16, characterized in that said encrypted communication path setting table holds a plurality of correspondences between the communication partner IP address and the intercept address.

18. A communication encryption node apparatus according to claim 16, characterized in that said name resolution proxy unit further comprises a communication method resolution unit which determines on the basis of the domain name of said other node apparatus whether said other node apparatus is the encrypted communication target node.

19. A communication encryption node apparatus according to claim 17, characterized in that

said encrypted communication path setting table holds encrypted communication path setting information to be used for communication with a communication partner in correspondence with the communication partner IP address and the intercept address,

said communication encryption unit reads out, from said encrypted communication path setting table, encrypted communication path setting information and the communication partner IP address corresponding to the intercept address set as the destination address of the received data packet, encrypts the data packet having

the readout communication partner IP address set as the destination address in accordance with the readout encrypted communication path setting information, and transmits the data packet,

said name resolution proxy unit further comprises a setting table which holds a correspondence between a domain name condition to specify an encrypted communication target node and encrypted communication path setting information,

said communication method resolution unit determines that said other node apparatus is the encrypted communication target node when the domain name of said other node apparatus matches any one of domain name conditions held in said setting table, and

said encrypted communication path setting unit registers, in said encrypted communication path setting table, encrypted communication path setting information corresponding to the matched domain name condition in correspondence with the IP address of said other node apparatus and the intercept address.

20. A communication encryption node apparatus according to claim 16, characterized in that said name resolution query/response transmission/reception unit transmits, to the name resolution server, the name resolution query transmitted from the application to resolve the IP address of said other node apparatus, receives, from the name resolution server, the name

resolution response containing a determination result indicating whether said other node apparatus is an encrypted communication target node and the IP address of said other node apparatus, and replaces the IP address of said other node apparatus contained in the name resolution response with the intercept address and transmits the name resolution response to the application if it is determined that said other node apparatus is the encrypted communication target node.

21. A communication encryption node apparatus according to claim 20, characterized in that

said encrypted communication path setting table holds encrypted communication path setting information to be used for communication with a communication partner in correspondence with the communication partner IP address and the intercept address,

said communication encryption unit reads out, from said encrypted communication path setting table, encrypted communication path setting information and the communication partner IP address corresponding to the intercept address set as the destination address of the received data packet, encrypts the data packet having the readout communication partner IP address set as the destination address in accordance with the readout encrypted communication path setting information, and transmits the data packet,

said name resolution query/response transmission/reception unit receives, from the name resolution server, the name resolution response further containing encrypted communication path setting information in addition to the determination result and the IP address of said other node apparatus, and

said encrypted communication path setting unit registers, in said encrypted communication path setting table, encrypted communication path setting information contained in the name resolution response in correspondence with the IP address of said other node apparatus and the intercept address.

22. A communication encryption node apparatus according to claim 18, characterized in that said communication method resolution unit determines whether said other node apparatus is an encrypted communication target node by looking up a setting table in which at least part of the domain name of the encrypted communication target node is registered.

23. An encrypted communication system characterized by comprising:

a node apparatus in which an application that communicates with another node apparatus connected to a network operates; and

a name resolution server which resolves an IP address of each of said node apparatuses,

said node apparatus comprising

a data transmission/reception unit provided in a kernel unit, and

a name resolution proxy unit which relays a name resolution query transmitted from the application to said name resolution server to resolve the IP address of said other node apparatus and a name resolution response as a response to the name resolution query,

said data transmission/reception unit comprising

an encrypted communication path setting table which holds a communication partner IP address, and

a communication encryption unit which receives a data packet transmitted from the application and encrypts and transmits the data packet when a communication partner IP address set as the destination address of the data packet is registered in said encrypted communication path setting table,

said name resolution server comprising a communication method resolution unit which determines on the basis of a domain name of said other node apparatus contained in one of the name resolution query and the name resolution response whether said other node apparatus is an encrypted communication target node, and

said name resolution proxy unit comprising an encrypted communication path setting unit which registers, in said encrypted communication path setting table, the IP address of said other node apparatus

resolved by the name resolution response if said other node apparatus is an encrypted communication target node.

24. An encrypted communication system according to claim 23, characterized in that said encrypted communication path setting table holds a plurality of communication partner IP addresses.

25. An encrypted communication system according to claim 23, characterized in that

said encrypted communication path setting table holds encrypted communication path setting information to be used for communication with a communication partner in correspondence with the communication partner IP address,

said communication encryption unit reads out corresponding encrypted communication path setting information from said encrypted communication path setting table, encrypts the data packet in accordance with the readout encrypted communication path setting information, and transmits the data packet when the communication partner IP address set as the destination address of the received data packet is registered in said encrypted communication path setting table,

said name resolution server comprises

a setting table which holds a correspondence between a domain name condition to specify an encrypted communication target node and encrypted communication

path setting information,

means, serving as said communication method resolution unit, for determining whether the domain name of said other node apparatus matches any one of domain name conditions held in said setting table, and

a name resolution query/response transmission/reception unit which adds encrypted communication path setting information corresponding to the matched domain name condition to the name resolution response and transmits the name resolution response, and

said encrypted communication path setting unit registers the encrypted communication path setting information in said encrypted communication path setting table in correspondence with the IP address of said other node apparatus upon receiving the name resolution response added the encrypted communication path setting information from said name resolution server.

26. An encrypted communication system according to claim 23, characterized in that said communication method resolution unit determines whether said other node apparatus is an encrypted communication target node by looking up a setting table in which at least part of the domain name of the encrypted communication target node is registered.

27. An encrypted communication system characterized by comprising:

a client node apparatus in which an

application that communicates with another node apparatus connected to a network operates;

a communication encryption node apparatus connected to said client node apparatus through the network; and

a name resolution server which resolves an IP address of each of said node apparatuses,

said communication encryption node apparatus comprising

a data transmission/reception unit provided in a kernel unit, and

a name resolution proxy unit which relays a name resolution query transmitted from the application to said name resolution server to resolve the IP address of said other node apparatus and a name resolution response as a response to the name resolution query,

said data transmission/reception unit comprising

an encrypted communication path setting table which holds a correspondence between a communication partner IP address and an intercept address, and

a communication encryption unit which receives a data packet transmitted from the application, reads out, from said encrypted communication path setting table, a communication partner IP address corresponding to an intercept address set as a destination address of the data packet, sets the readout communication partner

IP address as the destination address of the data packet, and encrypts and transmits the set data packet,

said name resolution server comprising a communication method resolution unit which determines on the basis of a domain name of said other node apparatus contained in one of the name resolution query and the name resolution response whether said other node apparatus is an encrypted communication target node, and

said name resolution proxy unit comprising

an encrypted communication path setting unit which registers, in said encrypted communication path setting table, a correspondence between the IP address of said other node apparatus resolved by the name resolution response and an intercept address that is not used in any other communication session if said other node apparatus is an encrypted communication target node, and

a name resolution query/response transmission/reception unit which transmits, to the application as the name resolution response, the intercept address corresponding to the IP address of said other node apparatus contained in the name resolution response received from the name resolution server.

28. An encrypted communication system according to claim 27, characterized in that said encrypted communication path setting table holds a

plurality of correspondences between the communication partner IP address and the intercept address.

29. An encrypted communication system according to claim 27, characterized in that

said encrypted communication path setting table holds encrypted communication path setting information to be used for communication with a communication partner in correspondence with the communication partner IP address and the intercept address,

said communication encryption unit reads out, from said encrypted communication path setting table, encrypted communication path setting information and the communication partner IP address corresponding to the intercept address set as the destination address of the received data packet, encrypts the data packet having the readout communication partner IP address set as the destination address in accordance with the readout encrypted communication path setting information, and transmits the data packet,

said name resolution server comprises

a setting table which holds a correspondence between a domain name condition to specify an encrypted communication target node and encrypted communication path setting information,

means, serving as said communication method resolution unit, for determining whether the domain name

of said other node apparatus matches any one of domain name conditions held in said setting table, and

a name resolution query/response transmission/reception unit which adds encrypted communication path setting information corresponding to the matched domain name condition to the name resolution response and transmits the name resolution response, and

said encrypted communication path setting unit registers the encrypted communication path setting information in said encrypted communication path setting table in correspondence with the IP address of said other node apparatus and the intercept address upon receiving the name resolution response added the encrypted communication path setting information from said name resolution server.

30. An encrypted communication system according to claim 27, characterized in that said communication method resolution unit determines whether said other node apparatus is an encrypted communication target node by looking up a setting table in which at least part of the domain name of the encrypted communication target node is registered.

31. A program which causes a computer included in a node apparatus in which an application that communicates with another node apparatus connected to a network operates to function as

communication encryption means provided in a

data transmission/reception unit of a kernel unit, and name resolution proxy means for relaying a name resolution query transmitted from the application to a name resolution server to resolve an IP address of said other node apparatus and a name resolution response as a response to the name resolution query, characterized in that

said communication encryption means receives a data packet transmitted from the application and encrypts and transmits the data packet when a communication partner IP address set as the destination address of the data packet is registered in an encrypted communication path setting table that holds a communication partner IP address, and

said name resolution proxy means comprises encrypted communication path setting means for registering, in the encrypted communication path setting table, the IP address of said other node apparatus resolved by the name resolution response if it is determined on the basis of a domain name of said other node apparatus contained in one of the name resolution query and the name resolution response that said other node apparatus is an encrypted communication target node.

32. A program according to claim 31, characterized in that the encrypted communication path setting table holds a plurality of communication partner

IP addresses.

33. A program according to claim 31, characterized in that said name resolution proxy means further comprise communication method resolution means for determining on the basis of the domain name of said other node apparatus whether said other node apparatus is an encrypted communication target node.

34. A program according to claim 33, characterized in that

the encrypted communication path setting table holds encrypted communication path setting information to be used for communication with a communication partner in correspondence with the communication partner IP address,

said communication encryption means reads out corresponding encrypted communication path setting information from said encrypted communication path setting table, encrypts the data packet in accordance with the readout encrypted communication path setting information, and transmits the data packet when the communication partner IP address set as the destination address of the received data packet is registered in said encrypted communication path setting table,

said communication method resolution means determines that said other node apparatus is an encrypted communication target node when the domain name of said other node apparatus matches any one of domain

name conditions held in a setting table that holds a correspondence between a domain name condition to specify an encrypted communication target node and encrypted communication path setting information, and

said encrypted communication path setting means registers, in the encrypted communication path setting table, encrypted communication path setting information corresponding to the matched domain name condition in correspondence with the IP address of said other node apparatus.

35. A program according to claim 31, characterized in that said name resolution proxy means further comprises name resolution query/response transmission/reception means for transmitting, to the name resolution server, the name resolution query transmitted from the application to resolve the IP address of said other node apparatus, receiving, from the name resolution server, the name resolution response containing a determination result indicating whether said other node apparatus is an encrypted communication target node and the IP address of said other node apparatus, and transmitting, to the application, the name resolution response containing the IP address of said other node apparatus contained in the name resolution response.

36. A program according to claim 35, characterized in that

the encrypted communication path setting table holds encrypted communication path setting information to be used for communication with a communication partner in correspondence with the communication partner IP address,

said communication encryption means reads out corresponding encrypted communication path setting information from the encrypted communication path setting table, encrypts the data packet in accordance with the readout encrypted communication path setting information, and transmits the data packet when the communication partner IP address set as the destination address of the received data packet is registered in the encrypted communication path setting table,

said name resolution query/response transmission/reception means receives, from the name resolution server, the name resolution response further containing encrypted communication path setting information in addition to the determination result and the IP address of said other node apparatus, and

said encrypted communication path setting means registers, in the encrypted communication path setting table, encrypted communication path setting information contained in the name resolution response in correspondence with the IP address of said other node apparatus.

37. A program according to claim 33,

characterized in that said communication method resolution means determines whether said other node apparatus is an encrypted communication target node by looking up a setting table in which at least part of the domain name of the encrypted communication target node is registered.

38. A program which causes a computer included in a communication encryption node apparatus connected, through a network, to a client node apparatus in which an application that communicates with another node apparatus connected to the network operates to function as

communication encryption means provided in a data transmission/reception unit of a kernel unit, and name resolution proxy means for relaying a name resolution query transmitted from the application to a name resolution server to resolve an IP address of said other node apparatus and a name resolution response as a response to the name resolution query, characterized in that

said communication encryption means receives a data packet transmitted from the application, reads out, from an encrypted communication path setting table that holds a correspondence between a communication partner IP address and an intercept address, a communication partner IP address corresponding to an intercept address set as a destination address of the data packet, sets

the readout communication partner IP address as the destination address of the data packet, and encrypts and transmits the set data packet, and

said name resolution proxy means comprises

encrypted communication path setting means for registering, in the encrypted communication path setting table, a correspondence between the IP address of said other node apparatus resolved by the name resolution response and an intercept address that is not used in any other communication session if it is determined on the basis of a domain name of said other node apparatus contained in one of the name resolution query and the name resolution response that said other node apparatus is an encrypted communication target node, and

name resolution query/response transmission/reception means for transmitting, to the application as the name resolution response, the intercept address corresponding to the IP address of said other node apparatus contained in the name resolution response received from the name resolution server.

39. A program according to claim 38, characterized in that the encrypted communication path setting table holds a plurality of correspondences between the communication partner IP address and the intercept address.

40. A program according to claim 38,

characterized in that said name resolution proxy means further comprises communication method resolution means for determining on the basis of the domain name of said other node apparatus whether said other node apparatus is the encrypted communication target node.

41. A program according to claim 40, characterized in that

the encrypted communication path setting table holds encrypted communication path setting information to be used for communication with a communication partner in correspondence with the communication partner IP address and the intercept address,

said communication encryption means reads out, from the encrypted communication path setting table, encrypted communication path setting information and the communication partner IP address corresponding to the intercept address set as the destination address of the received data packet, encrypts the data packet having the readout communication partner IP address set as the destination address in accordance with the readout encrypted communication path setting information, and transmits the data packet,

said communication method resolution means determines that said other node apparatus is an encrypted communication target node when the domain name of said other node apparatus matches any one of domain name conditions held in a setting table that holds a

correspondence between a domain name condition to specify an encrypted communication target node and encrypted communication path setting information, and

said encrypted communication path setting means registers, in the encrypted communication path setting table, encrypted communication path setting information corresponding to the matched domain name condition in correspondence with the IP address of said other node apparatus and the intercept address.

42. A program according to claim 38, characterized in that said name resolution query/response transmission/reception means transmits, to the name resolution server, the name resolution query transmitted from the application to resolve the IP address of said other node apparatus, receives, from the name resolution server, the name resolution response containing a determination result indicating whether said other node apparatus is an encrypted communication target node and the IP address of said other node apparatus, and replaces the IP address of said other node apparatus contained in the name resolution response with the intercept address and transmits the name resolution response to the application if it is determined that said other node apparatus is the encrypted communication target node.

43. A program according to claim 42, characterized in that

the encrypted communication path setting table holds encrypted communication path setting information to be used for communication with a communication partner in correspondence with the communication partner IP address and the intercept address,

said communication encryption means reads out, from the encrypted communication path setting table, encrypted communication path setting information and the communication partner IP address corresponding to the intercept address set as the destination address of the received data packet, encrypts the data packet having the readout communication partner IP address set as the destination address in accordance with the readout encrypted communication path setting information, and transmits the data packet,

said name resolution query/response transmission/reception means receives, from the name resolution server, the name resolution response further containing encrypted communication path setting information in addition to the determination result and the IP address of said other node apparatus, and

said encrypted communication path setting means registers, in the encrypted communication path setting table, encrypted communication path setting information contained in the name resolution response in correspondence with the IP address of said other node apparatus and the intercept address.

44. A program according to claim 40, characterized in that said communication method resolution means determines whether said other node apparatus is an encrypted communication target node by looking up a setting table in which at least part of the domain name of the encrypted communication target node is registered.